CLAIMS

We claim:

1. A method comprising:

generating a first key component;

generating an encryption key using the first key component, a token key and a personal identification number (PIN);

encrypting data using the encryption key;

sending the data encrypted with the encryption key to a server along with the first key component.

2. The method defined in Claim 1 further comprising receiving the token key from a service provider.

3. The method defined in Claim 1 further comprising the server storing the first key component and the data encrypted with the encryption key.

4. The method defined in Claim 1 wherein the token key is unique for each user.

5. The method defined in Claim 1 wherein the first key component is unique for each data entry stored by the server.

6. A method comprising:

encrypting data using the encryption key generating using a first key component, a token key and a personal identification number (PIN);

storing data encrypted using the encryption key; and

regenerating the encryption key after accessing the encrypted data to decrypt the encrypted data therewith.

7. The method defined in Claim 6 further comprising disabling the token.

8. The method defined in Claim 7 wherein the token is disabled if lost.

9. The method defined in Claim 7 wherein the token is disabled if compromised.

10. The method defined in Claim 7 further comprising re-enabling the token.

11. The method defined in Claim 6 wherein the token ID comprises an alpha-numeric string.

12. The method defined in Claim 11 wherein the token key comprises a randomly generated number.

13. The method defined in Claim 11 wherein either or both of the token key and PIN comprises biometric data.

14. The method defined in Claim 11 wherein the token key is the same for all tokens used by the user.

15. The method defined in Claim 6 further comprising:

monitoring browsing activities;

identifying web pages containing a form; and

inserting content into the form.

16. The method defined in Claim 15 wherein inserting content into the form is performed automatically.

17. The method defined in Claim 15 wherein inserting content into the form is performed with user confirmation.

18. The method defined in Claim 15 further comprising allowing a user to select the form to fill in.

19. The method defined in Claim 15 further comprising allowing a user to select a variant of the form to fill in.

20. A method comprising:

retrieving a key component and encrypted data from a server;

recreating an encryption key using the key component, a token key and a personal identification number (PIN); and

performing a decryption operation on the encrypted data using a decryption key based on the encryption key used to encrypt the encrypted data.

21. A method for authentication comprising:

generating authentication data for a user based on a token key and a personal identification number (PIN), the token key being unique to the user; and

receiving a confirmation indicating that the authentication data has been verified.

22. A method comprising:

accessing encrypted data from a server;

decrypting the encrypted data using a token and a user-specific PIN to be accessed.

23. The method defined in Claim 22 wherein the token comprises a token identifier (ID) and a token key.

24. The method defined in Claim 22 wherein the token comprises a utility to manage data depending on data type.

25. The method defined in Claim 24 wherein the utility operates on data in response to explicit user command or by automatically monitoring applications producing and/or consuming data of that type.

26. The method defined in Claim 25 wherein the utility handles password data.